NIST Special Publication 800-137

Information Security Continuous Monitoring for Federal Information Systems and Organizations

Holistic Continuous Monitoring and CAESARS FE

NIST Continuous Monitoring Architecture Workshop

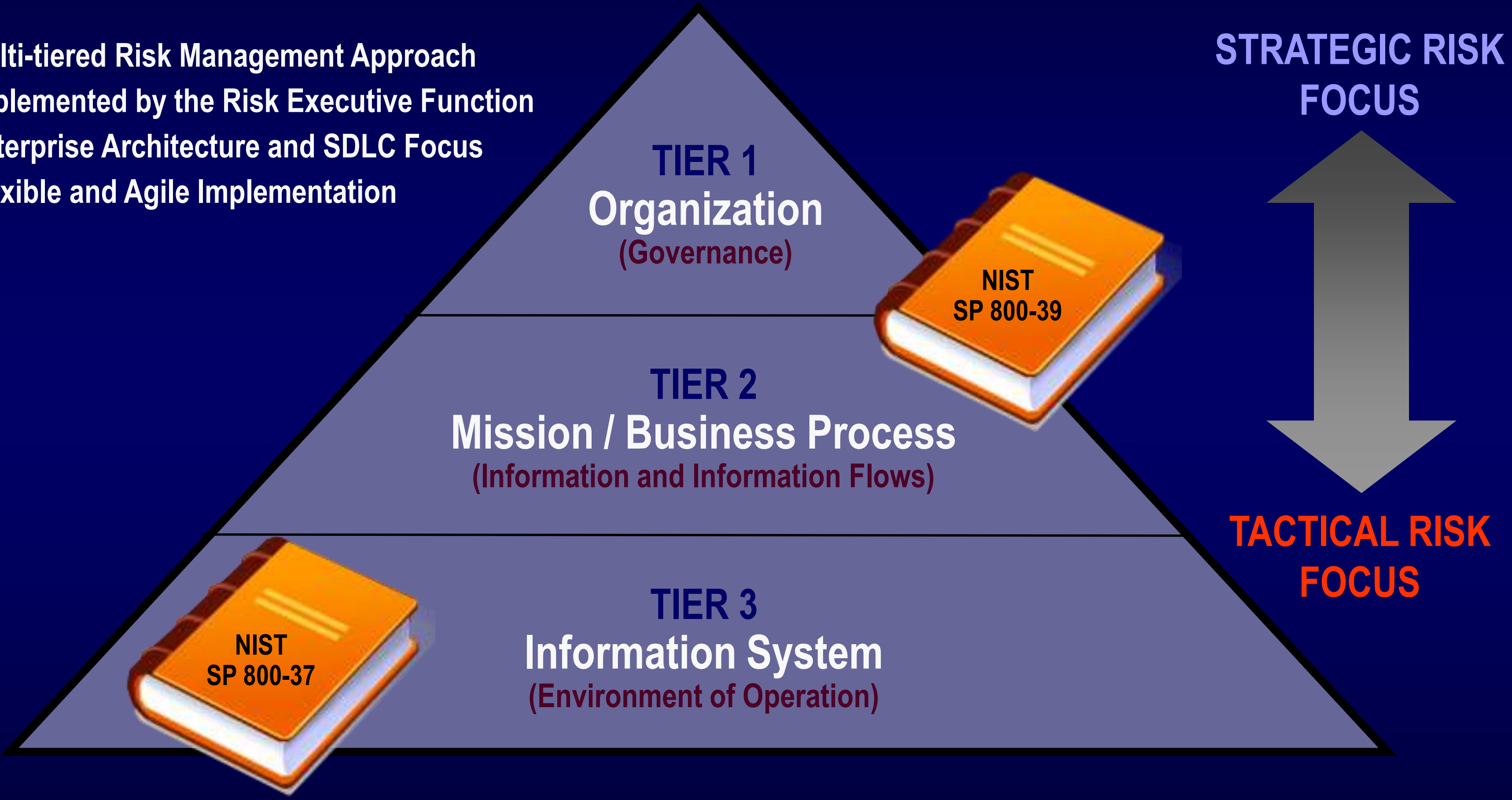
March 21, 2011

Kelley Dempsey

Computer Security Division
Information Technology Laboratory

Enterprise-Wide Risk Management

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation



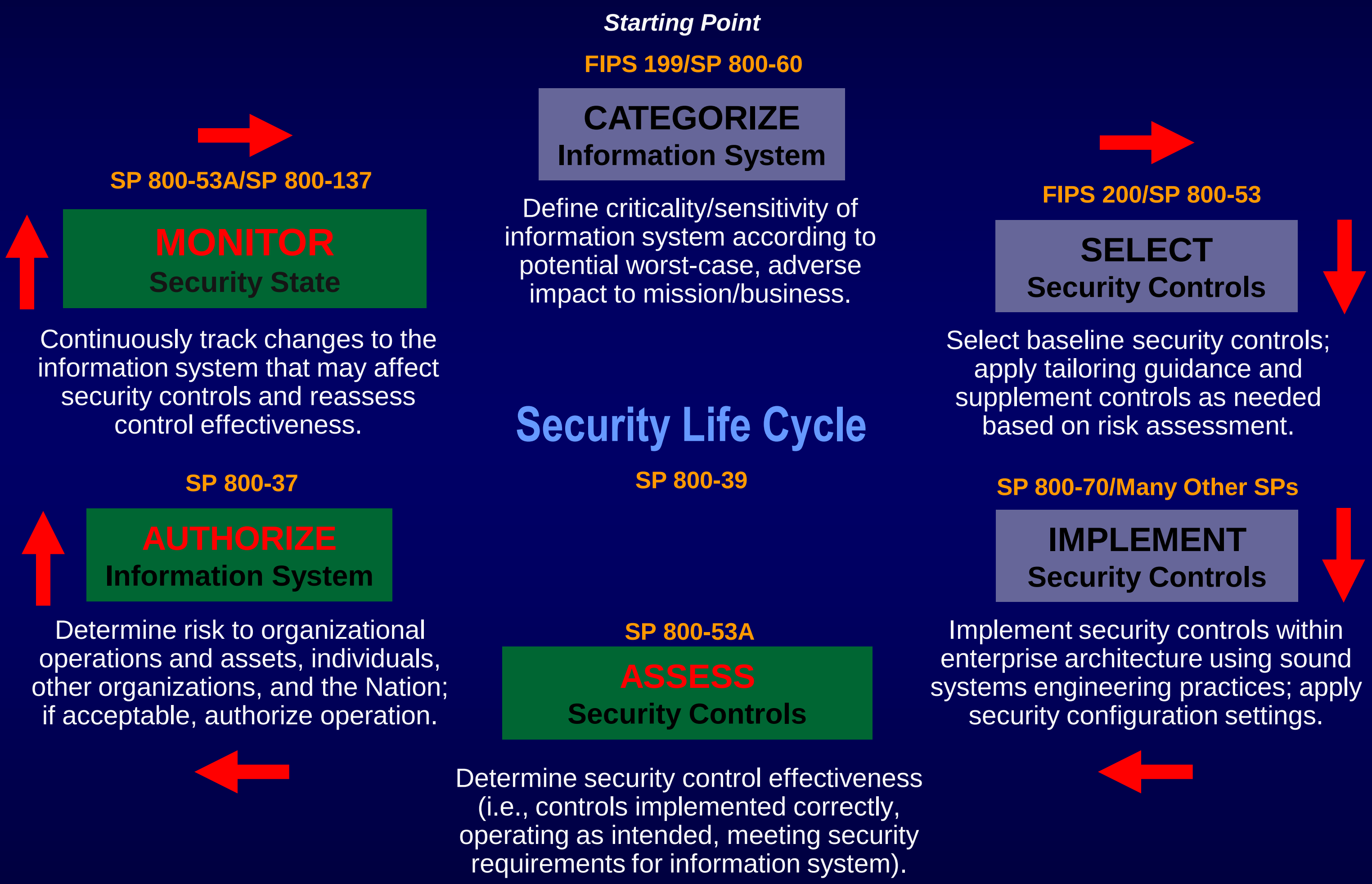
Characteristics of Risk-Based Approaches
(1 of 2)

- Promotes near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes.
- Integrates information security more closely into the system development life cycle.
- Links risk management processes at the information system level to risk management processes at the organization level through a risk executive (function).

Characteristics of Risk-Based Approaches
(2 of 2)

- Encourages the use of automation to increase consistency, effectiveness, and timeliness of security control implementation and functionality
- Provide senior leaders the necessary information to make credible, risk-based decisions with regard to the information systems supporting their core missions and business functions
- Establishes responsibility and accountability for security controls deployed within information systems.

Continuous Monitoring & the RMF



Starting Point

FIPS 199/SP 800-60

CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 200/SP 800-53

SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

SP 800-70/Many Other SPs

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-53A

ASSESS
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-37

AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-53A/SP 800-137

MONITOR
Security State

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life Cycle

SP 800-39

Continuous Monitoring Definition

- Continuous* monitoring (generic) is maintaining ongoing awareness to support organizational risk decisions.
- Information security continuous* monitoring is maintaining ongoing* awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

* The terms “continuous” and “ongoing” in this context mean that security controls and organizational risks are assessed, analyzed and reported at a frequency sufficient to support risk-based security decisions as needed to adequately protect organization information.

Continuous Monitoring Objectives

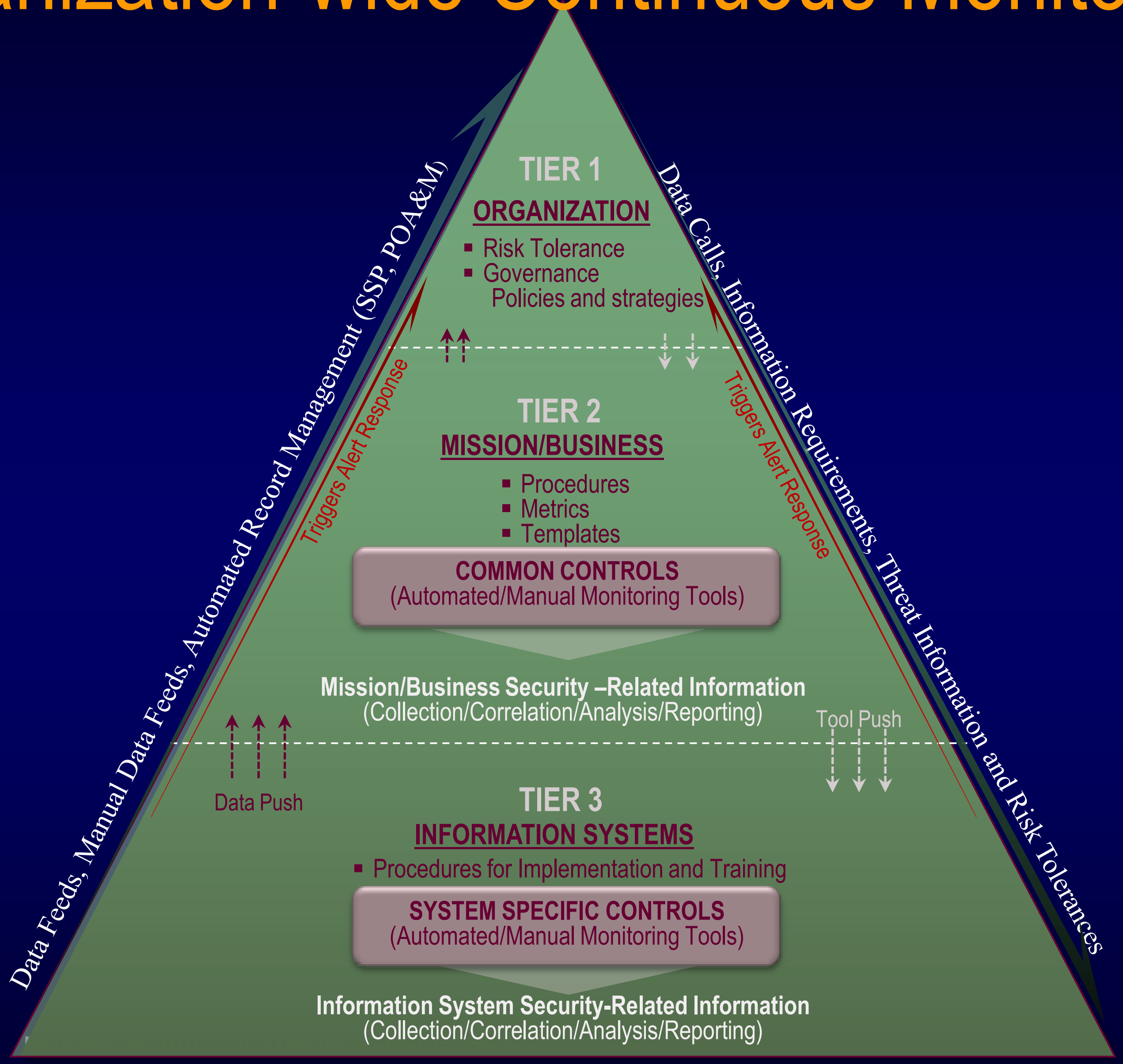
- Conduct **ongoing monitoring of the security** of an organization's information, applications, networks, and systems, and **respond to risk** as situations change.
- Determine if the **security controls** implemented within an information system or inherited by the system **continue to be effective over time** in light of the inevitable changes that occur.
- Ensure monitoring and reporting frequencies remain aligned with threats and organizational risk tolerance by **monitoring the monitoring strategy itself.**

Precursors to NIST SP 800-137

The Continuous Monitoring Process, as described in NIST SP 800-137, is consistent with and an expansion of:

- Step Six of the Risk Management Framework (NIST SP 800-37 Revision 1)
- Appendix G of NIST SP 800-37 Revision 1
- Control CA-7 from NIST SP 800-53 Revision 3

Organization-wide Continuous Monitoring



TIER 1

ORGANIZATION

- Risk Tolerance
- Governance

  Policies and strategies

TIER 2

MISSION/BUSINESS

- Procedures
- Metrics
- Templates

COMMON CONTROLS
(Automated/Manual Monitoring Tools)

Mission/Business Security –Related Information
(Collection/Correlation/Analysis/Reporting)

TIER 3

INFORMATION SYSTEMS

- Procedures for Implementation and Training

SYSTEM SPECIFIC CONTROLS
(Automated/Manual Monitoring Tools)

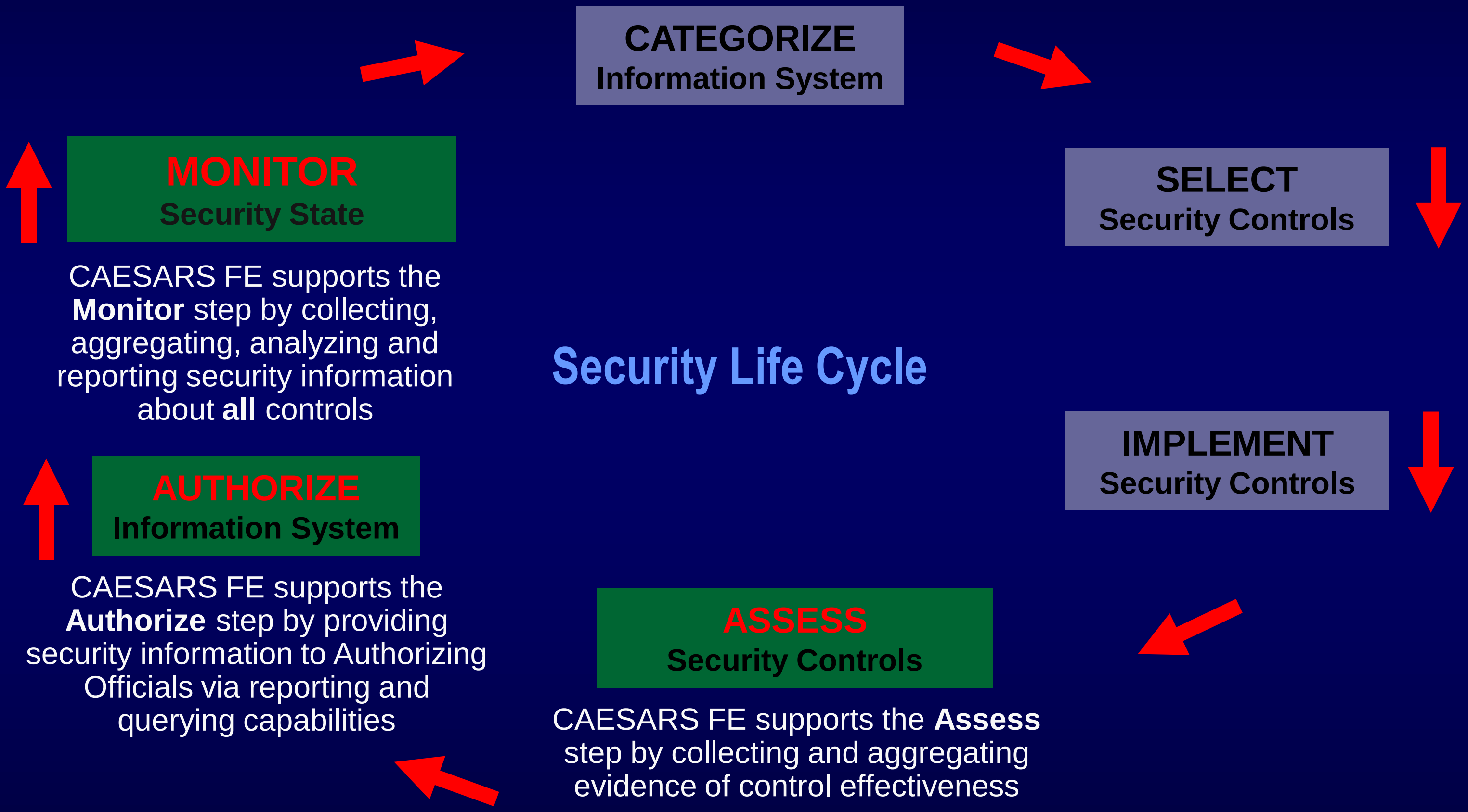
Information System Security-Related Information
(Collection/Correlation/Analysis/Reporting)

Data Feeds, Manual Data Feeds, Automated Record Management (SSP, POA&M)
Data Calls, Information Requirements, Threat Information and Risk Tolerances
Triggers Alert Response
Triggers Alert Response
Data Push
Tool Push

Technologies for Enabling Continuous Monitoring

- Direct data gathering
  - Eleven security domains
- Aggregation and analysis
  - Security information and event management (SIEM)
  - Management dashboards
- Automation and Data Sources
  - Security content automation protocol (SCAP), XML, etc.
  - Data sources

CAESARS Framework Extension (FE) Support of the RMF



CATEGORIZE
Information System

SELECT
Security Controls

IMPLEMENT
Security Controls

ASSESS
Security Controls

CAESARS FE supports the **Assess** step by collecting and aggregating evidence of control effectiveness

AUTHORIZE
Information System

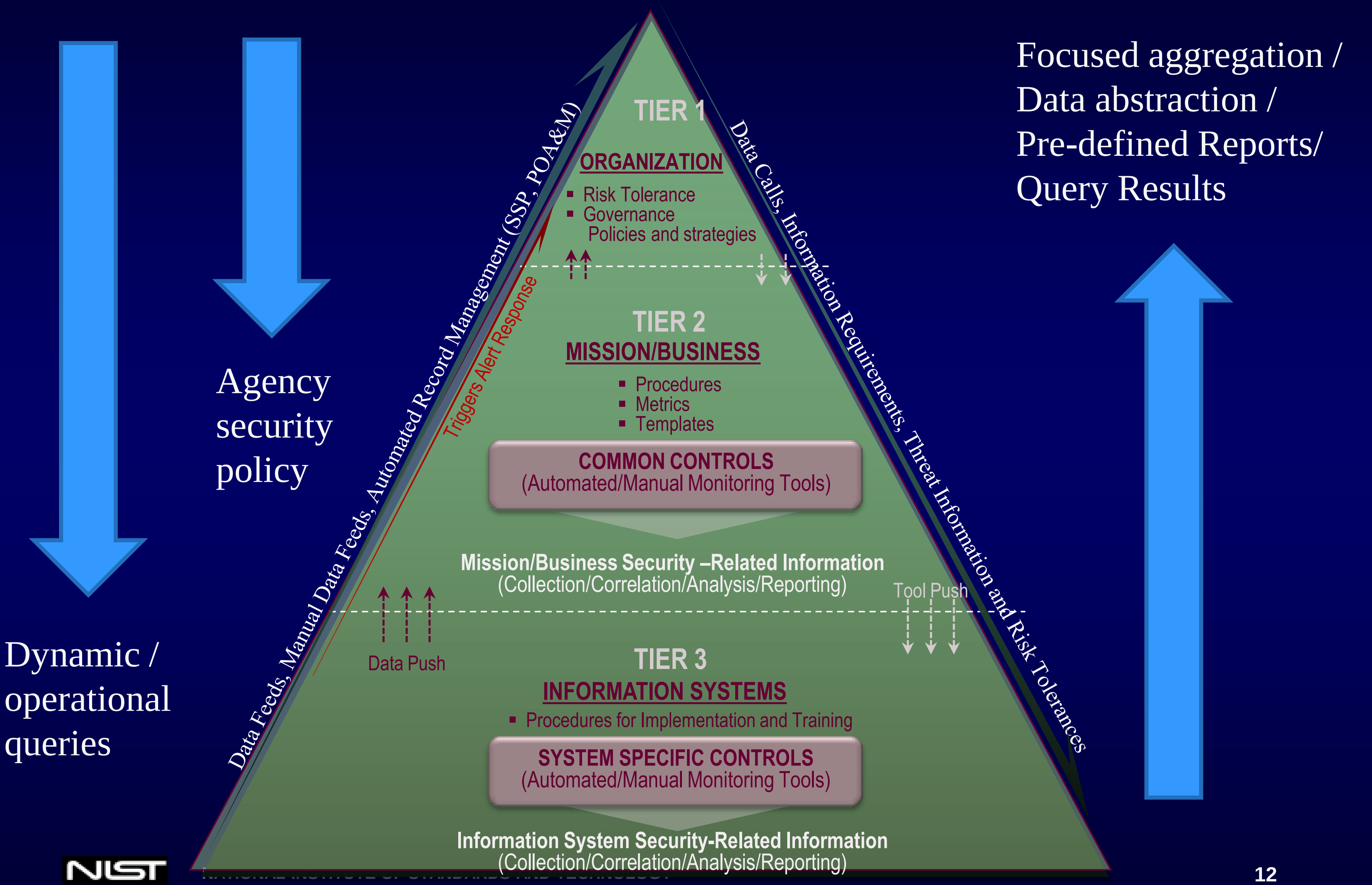
CAESARS FE supports the **Authorize** step by providing security information to Authorizing Officials via reporting and querying capabilities

MONITOR
Security State

CAESARS FE supports the **Monitor** step by collecting, aggregating, analyzing and reporting security information about **all** controls

Security Life Cycle

CAESARS FE Supports CoMo at All Three Tiers



Agency security policy

Dynamic / operational queries

Focused aggregation / Data abstraction / Pre-defined Reports/ Query Results

Data Feeds, Manual Data Feeds, Automated Record Management (SSP, POA&M)

Triggers Alert Response

Data Calls, Information Requirements, Threat Information and Risk Tolerances

TIER 1

ORGANIZATION

- Risk Tolerance
- Governance
  Policies and strategies

TIER 2

MISSION/BUSINESS

- Procedures
- Metrics
- Templates

COMMON CONTROLS
(Automated/Manual Monitoring Tools)

Mission/Business Security –Related Information
(Collection/Correlation/Analysis/Reporting)

Tool Push

Data Push

TIER 3

INFORMATION SYSTEMS

- Procedures for Implementation and Training

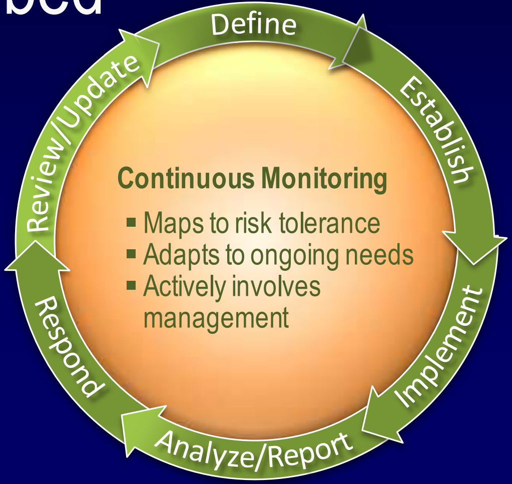
SYSTEM SPECIFIC CONTROLS
(Automated/Manual Monitoring Tools)

Information System Security-Related Information
(Collection/Correlation/Analysis/Reporting)

CAESARS FE can provide layer relevant data

Continuous Monitoring Process Steps

The Continuous Monitoring process, as described in NIST SP 800-137, consists of seven steps:



- Define strategy
- Establish measures and metrics
- **Establish monitoring frequencies**
- **Implement the monitoring program**
- **Analyze security-related information (data) and report findings**
- Respond with mitigation actions OR reject/avoid, transfer, or accept risk
- **Review and update monitoring strategy and program**

CAESARS FE

CAESARS FE Support for CoMo Step 3

Establish Monitoring and Assessment Frequencies

- 800-137 Guidance: Monitor metrics/measures and **each** control with varying frequencies
  - CAESARS FE supports monitoring at varying frequencies in accordance with the specific requirements and risk tolerance at each organization
  - Continual vs. Continuous (periodicity from milliseconds to years)

CAESARS FE Support for CoMo Step 4

Implement the Continuous Monitoring Program

- The CAESARS FE model can support full achievement of the implementation step
- CAESARS FE supports monitoring of **all** controls regardless of input method (i.e., manual or automated)
  - The necessary data standards must exist for the applicable data domains!!
- CAESARS FE is **NOT** only focused on technical control evaluation
  - Example 1: CAESARS FE could leverage an 800-53 control XML representation
  - Example 2: CAESARS FE could leverage a POAM XML representation

CAESARS FE Support of CoMo Step 5

Analyze Data and Report Findings

- Supports varying degrees of granularity for different report recipients:
  - Core capabilities – Pre-defined reports (views) tailored for organizational requirements (e.g., the three tiers)
    - Different views for operations, decision makers, and compliance reports
  - Advanced capabilities – Dynamic/selective querying from Tier 1 down
    - Eliminates need for agencies to aggregate **all** low level data up to the agency level
      - Reduces security risk and minimizes storage/network throughput issues
  - CAESARS FE supports dynamic adjustment of scoring algorithms, parameters, and weights

CAESARS FE Support for CoMo Step 7

Review and Update Monitoring Strategy and Programs

- CAESARS FE supports dynamic adjustment of scoring algorithms, parameters, and weights
  - Use reports, queries, and scoring information to examine trends, determine if frequencies and metrics are appropriate, etc.

Continuous Monitoring Automation:
The Need for Caution (1 of 2)

- Automation of monitoring using standard reference architectures (e.g., CAESARS FE) ***supports*** holistic monitoring and ***is strongly encouraged***, but…
- The security-related information generated via automated tools is not the end of the story:
  - Agencies evaluate and act upon the data based on a well-defined risk management process (SP 800-39)
  - The tools themselves have to be monitored for accuracy and integrity on a regular basis

Continuous Monitoring Automation:

The Need for Caution (2 of 2)

Automated tools may lead to a false sense of security:

- If **all** controls are **not** taken into account when monitoring, an **incomplete picture of overall security posture** and risk is presented:
  - Risk scores may not be comprehensive, i.e., an automated tool cannot score risks about which it has no information
  - Risk scoring is often based solely on automation of technical controls and thus is not a substitute for monitoring other essential operational and management controls nor can it determine how security failures will affect organization functions and mission

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov